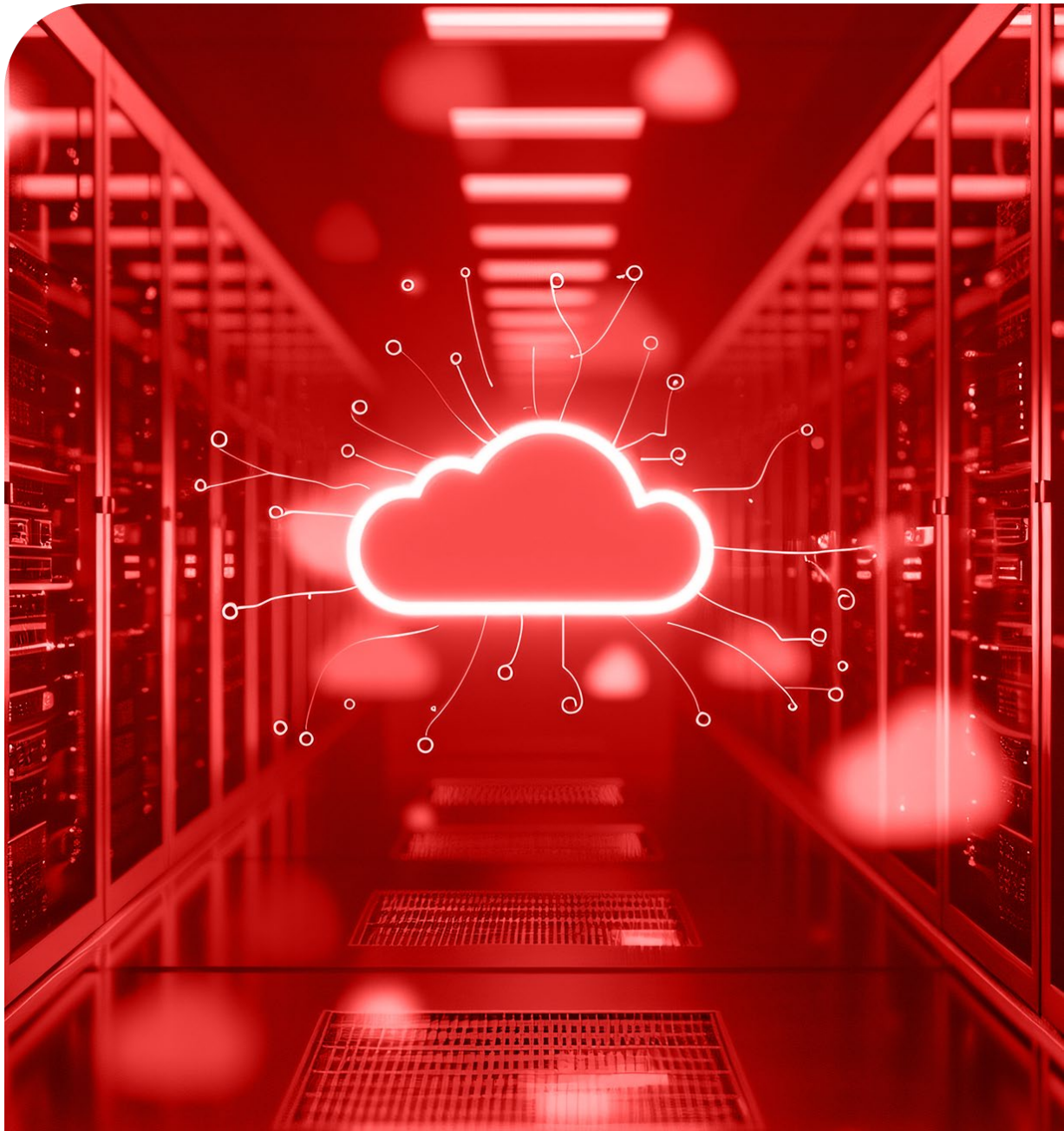
Synoptek

Case Study

Strengthening Identity and Cloud Security in a Hybrid Microsoft Environment



Customer Overview

Customer

A leading provider of memorial and end-of-life services

Profile

The organization operates a network of memorial parks and service locations, supporting individuals and families with planning and coordination services across multiple sites.

Industry

Consumer Services

Services

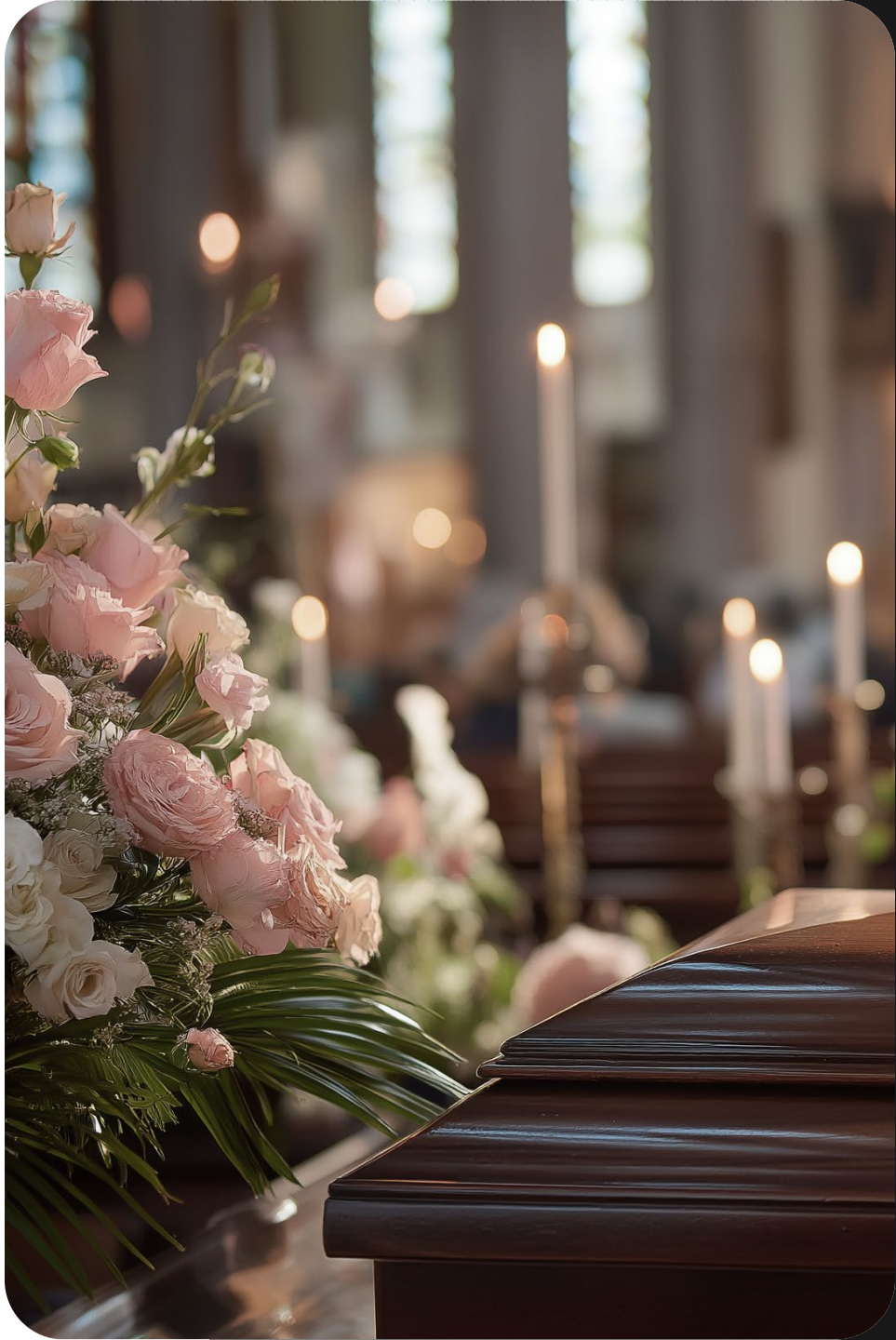
Cloud Security Assessment | Identity & Access Management (IAM) | Microsoft 365 Security | Endpoint Security | Governance & Compliance | Zero Trust Enablement

Business Need

As the organization expanded its use of Microsoft Cloud services, it faced increasing challenges in managing identity, access, and security configurations across a complex environment. Without a structured security baseline, the organization required greater visibility, governance, and control to mitigate growing cyber risks.

Key requirements included:

- Establish a baseline security posture across Microsoft 365 and Entra ID
- Improve visibility into privileged access and identity configurations
- Strengthen governance for users, applications, and service principals
- Ensure consistent enforcement of endpoint security policies
- Align security controls with Zero Trust principles
- Reduce risk of identity-based attacks and unauthorized access



Approach

Synoptek conducted a structured Microsoft cloud security assessment to evaluate identity, access, and endpoint security controls, and to define a prioritized roadmap for strengthening the organization’s security posture.

Discovery & Data Collection

Collected and analyzed configuration data across Microsoft 365 and Entra ID, including users, groups, roles, applications, permissions, and audit logs to establish a complete inventory of identity and access relationships.

Identity Governance Review

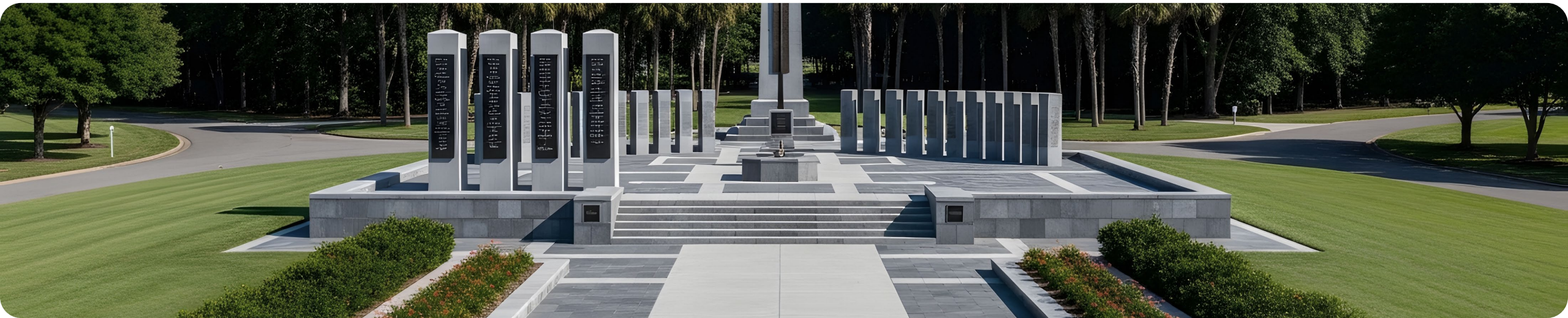
Assessed governance controls for application registrations, OAuth permissions, enterprise applications, guest access, and conditional access policies to identify gaps and improve access management practices.

Privileged Access & Risk Analysis

Evaluated administrative roles, privileged access assignments, and service principal permissions to identify risks such as privilege sprawl, excessive permissions, and potential escalation paths.

Cloud Configuration Assessment

Reviewed Microsoft 365 tenant configuration, licensing, audit logging, and administrative structures to evaluate alignment with available security capabilities and best practices.



Approach

Endpoint Security Evaluation

Analyzed device management, compliance policies, endpoint configurations, and mobile device management to identify inconsistencies and opportunities to strengthen endpoint security posture.

Security Monitoring & Visibility Enhancements

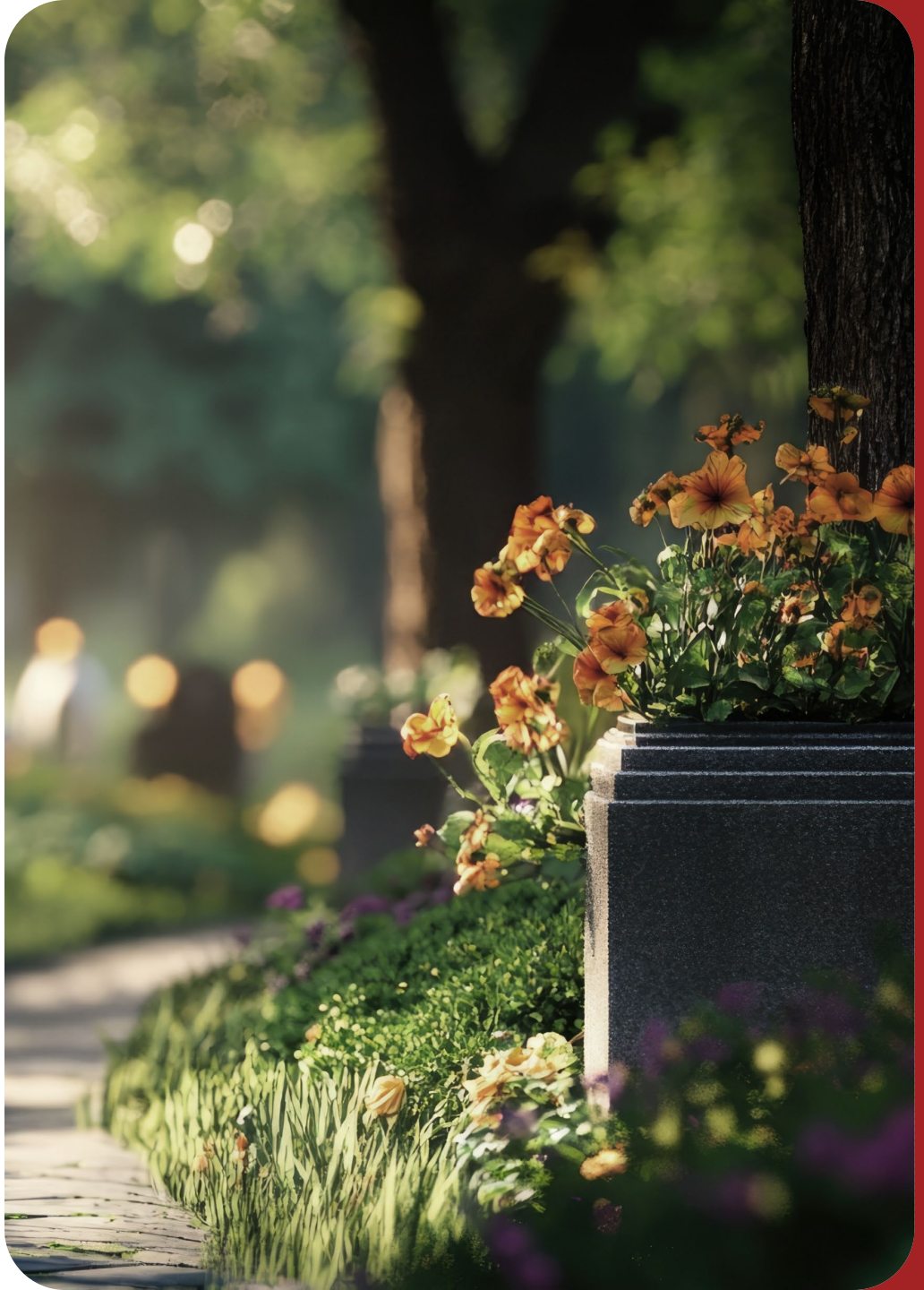
Identified opportunities to improve monitoring by centralizing audit logs and enhancing correlation with security tools for better detection and response.

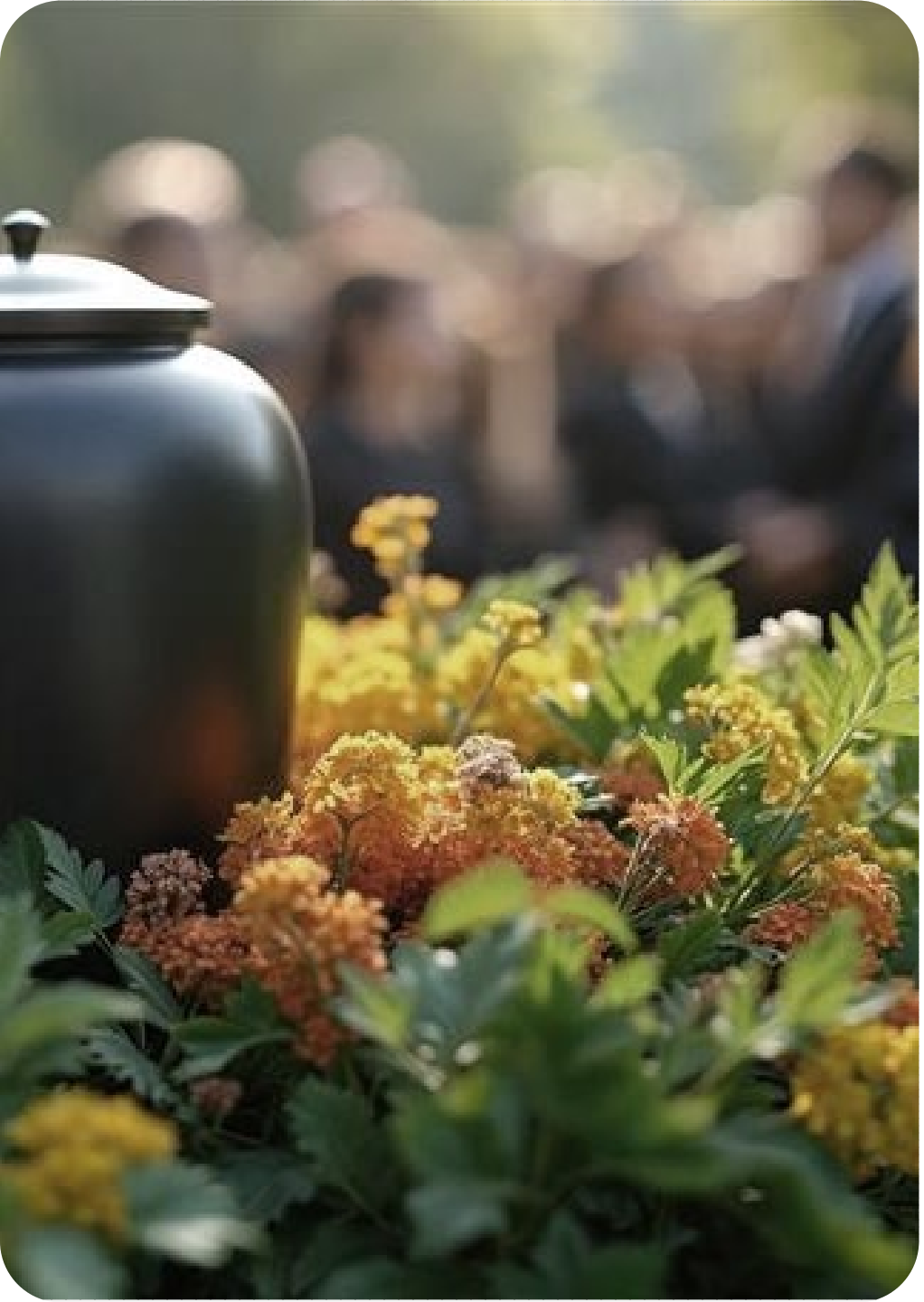
Governance & Control Framework

Recommended structured governance models for identity lifecycle management, application ownership, and privileged access controls.

Zero Trust Alignment

Aligned all findings and recommendations with Zero Trust principles, focusing on identity as the core control plane for securing access and reducing attack surfaces.





Key Outcomes

The assessment provided the organization with a clear understanding of its current security posture and actionable recommendations for improvement.

- Comprehensive visibility into identity, access, and privileged relationships
- Identification of security gaps and misconfigurations across the environment
- Defined roadmap for identity governance and access control improvements
- Alignment of security controls with modern frameworks and Zero Trust principles
- Improved understanding of application access and permission risks

Business Impact

By addressing identity and access control gaps, the organization strengthened its security foundation and reduced potential risk exposure.

Improved control over privileged access and administrative roles

Strengthened governance across applications, users, and access policies

Reduced risk of unauthorized access and privilege escalation

Enhanced consistency in endpoint security and compliance enforcement

Improved monitoring and visibility for faster threat detection

Established a scalable foundation for ongoing security improvements

About Synoptek

Synoptek is the first IT Managed Experience Provider (MxP™), delivering AI-enabled automation, strategic modernization, and experience-led outcomes. Its services span Cloud and Agile Infrastructure, Business Applications and Platform Development, Customer and Employee Experience, and Cybersecurity. With a business-first approach and a global delivery model, Synoptek helps organizations optimize operations, accelerate transformation, and achieve measurable results—guided by a culture rooted in growth, ownership, inclusiveness, and philanthropy.

Synoptek

Pacific Arts Plaza, 611 Anton Blvd., Suite #925,
Costa Mesa, CA 92626

303-728 3335

salesinquiries@synoptek.com

www.synoptek.com